OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

March 26, 2014

Fiscal Year 2013 Information Technology Internal Controls

Report Number IT-AR-14-003

BACKGROUND:

The Postal Accountability and Enhancement Act of 2006 requires the U.S. Postal Service to comply with the Sarbanes-Oxley Act and make an assertion on the effectiveness of the internal control structure over financial reporting. We conducted this audit in support of the independent public accounting firm's overall audit opinions on the Postal Service's financial statements and internal controls over financial reporting.

The Information Technology system-level environment includes processes needed to administer, secure, and monitor key financial systems. Our objective was to evaluate and test key system-level internal controls over information systems.

WHAT THE OIG FOUND:

The system-level internal controls we tested were properly designed and generally operating effectively. For example, database software controls functioned properly when we tested password security settings and updates. However, we identified opportunities to strengthen certain controls, which would reduce the risk information technology resources would be compromised. Specifically, these improvements would help control owners better manage change management policies and job scheduling procedures for the [redacted] and strengthen administrator access controls for workload scheduling software.

Management also took corrective action to address eight additional issues identified during our audit. We also confirmed management took corrective actions to address 15 prior year issues and is currently remediating 12 other issues reported during fiscal years 2010 through 2012.

We discussed related causes and recommended actions to improve the control environments. The control weaknesses identified, alone or collectively, do not prevent reliance on system-level internal controls for accurate and timely financial reporting.

Corrective actions can reduce the risk of a compromise that could harm the confidentiality, integrity, and availability of information resources.

WHAT THE OIG RECOMMENDED:

We recommended management ensure [redacted] administrators follow job control policies and implement a job scheduling procedure. We also recommended management properly document changes to computer command lists and require a password expiration setting for the workload automation software.